UET.SIR: Giải pháp hỗ trợ xử lý sự cố an toàn thông tin trong chính phủ điện tử

Lê Hồng Hải, Tống Minh Đức, Ngô Quang Huy, Phùng Văn Ổn, Nguyễn Ngọc Hóa

***Tóm tắt*— Bài báo này trình bày kết quả nghiên cứu xây dựng giải pháp hỗ trợ xử lý sự cố an toàn thông tin (ATTT) phục vụ tổ chức trong Chính phủ điện tử. Giải pháp đề xuất bao gồm cả quy trình xử lý sự cố ATTT và hệ thống UET.SIR phục vụ công tác hỗ trợ xử lý sự cố ATTT. Quy trình được xây dựng dựa trên kết hợp các tiêu chuẩn trong nước và quốc tế, được tuỳ biến để phù hợp với thực tiễn của chính phủ điện tử. Hệ thống UET.SIR hỗ trợ xử lý xự cố bao gồm USB chuyên dụng phục vụ thu thập chứng cứ số sự cố ATTT, và phần mềm trung tâm với các chức năng phân tích chứng cứ sự cố để phát hiện nguyên nhân và hỗ trợ công tác xử lý. Kết quả thử nghiệm hệ thống UET.SIR tại Bộ Tài nguyên và Môi trường bước đầu đã chứng minh được khả năng áp dụng thực tiễn và hỗ trợ xử lý sự cố ATTT đối với một số hệ thống trọng yếu.**

***Abstract*— This paper presents the results of research on building solutions to support information security incident handling in organizations. The proposed solution includes both the procedure for information security incident handling, and the UET.SIR system for supporting information security handling. The process is built on a combination of national and international standards, but is customized to suit e-government practices. The UET.SIR system includes a dedicated USB for collecting digital evidence of ATTT incidents and central software with evidence analysis functions to detect the cause and provide support incident handling. The test results of the UET.SIR system at the Ministry of Natural Resources and Environment have initially demonstrated its practical applicability and support for information security incident handling.**

Từ khóa*— *sự cố ATTT; thu thập chứng cứ sự cố; xử lý sự cố ATTT.

Keywords*— *information security incident; information security incident evidence; information security incident handling.

Bài báo được nhận ngày 13/4/2022. Bài báo được nhận xét bởi phản biện thứ nhất ngày 23/5/2022 và được chấp nhận đăng ngày 30/5/2022. Bài báo được nhận xét bởi phản biện thứ hai ngày 25/5/2022 và được chấp nhận đăng ngày 03/6/2022.

I. ĐẶT VẤN ĐỀ

Khi triển khai Chính phủ điện tử, các hệ thống công nghệ thông tin (CNTT) đóng vai trò đặc biệt quan trọng, bảo đảm cho sự hoạt động của Chính phủ hiệu quả và chúng cần được duy trì liên tục và ổn định. Bên cạnh quá trình giám sát và đánh giá rủi ro hệ thống [2], khi các hệ thống CNTT này gặp sự cố, cần thiết phải được xử lý, khắc phục một cách chủ động, kịp thời. Nghiên cứu này nhằm đề xuất giải pháp hỗ trợ xử lý sự cố an toàn cho các hệ thống CNTT trong Chính phủ điện tử của Việt Nam. Sự cố an toàn thông tin có thể gây ra những tổn thất nặng nề về kinh tế cho tổ chức, doanh nghiệp, thậm chí ảnh hưởng nghiêm trọng đến an ninh quốc gia. Các sự cố ATTT thường liên quan đến việc khai thác các lỗ hổng chưa được phát hiện và/hoặc không được kiểm soát, do đó việc xử lý sự cố có vai trò đặc biệt quan trọng trong hoạt động bảo đảm ATTT. Để xử lý sự cố ATTT một cách hiệu quả, chúng ta phải có những biện pháp thu thập, điều tra, phát hiện nguyên nhân để khắc phục nhanh sự cố; từ đó mới có thể giảm thiểu tác động bất lợi hoặc tổn thất do sự cố gây ra. Mặc dù trên thế giới hiện đã có nhiều tổ chức nghiên cứu và các doanh nghiệp cung cấp những giải pháp hỗ trợ công tác bảo đảm ATTT nói chung và xử lý sự cố ATTT nói riêng, tuy nhiên với mỗi quốc gia, bao gồm cả Việt Nam, rất cần làm chủ được công nghệ và có giải pháp của riêng mình để chủ động trong công tác bảo đảm an ninh thông tin quốc gia và đó cũng là mục tiêu chính của nghiên cứu này.

Trong nghiên cứu này, nhóm tác giả tập trung xây dựng giải pháp hỗ trợ công tác xử lý sự cố ATTT cho các hệ thống CNTT nói chung và trong Chính phủ điện tử nói riêng. Giải pháp này bao gồm cả quy trình phục vụ cho việc thu thập, phân tích, xử lý sự cố ATTT và hệ thống phần mềm đảm nhiệm vai trò tương ứng. Hệ thống này bao gồm (i) USB chuyên dụng kèm theo công cụ phần mềm phục vụ thu thập chứng cứ sự cố

ATTT; (ii) Một phần mềm trung tâm phục vụ cho việc quản lý, phân tích những chứng cứ sự cố thu thập được, xác định nguyên nhân sự cố, trên cơ sở đó sẽ hỗ trợ chuyên gia xây dựng phương án xử lý sự cố tương ứng.

Bài báo này được phát triển mở rộng từ bài đăng kỷ yếu hội thảo [17]. Phần còn lại của bài báo được tổ chức như sau: Phần II tóm lược một số phương pháp, kỹ thuật sử dụng trong xử lý sự cố ATTT; Phần III trình bày giải pháp xử lý sự cố ATTT của nhóm tác giả đã xây dựng trong khuôn khổ đề tài cấp nhà nước KC.01.19/16-20; Phần IV tổng hợp kết quả thử nghiệm giải pháp; Phần V tóm lược kết quả và một số hướng phát triển tiếp theo.

II. PHƯƠNG PHÁP, KỸ THUẬT HỖ TRỢ XỬ LÝ SỰ CỐ ATTT

Trong phần này, nhóm tác giả tóm lược các phương pháp, kỹ thuật được sử dụng trong hoạt động xử lý sự cố an toàn thông tin.

A. Chứng cứ số sự cố ATTT

Chứng cứ số sự cố ATTT hay còn gọi tắt là chứng cứ số, là các thông tin, dữ liệu trong dạng số được thu thập, lưu trữ theo trình tự thủ tục quy định và có giá trị pháp lý, được sử dụng làm căn cứ để phân tích, điều tra xác định nguyên nhân, nguồn gốc sự cố. Chứng cứ số được thể hiện qua hai hình thức là vật lý (chứng cứ biểu diễn của dữ liệu trong một thiết bị hữu hình - vật tải dữ liệu) và logic (chứng cứ số tiềm năng chỉ các biểu diễn ảo của dữ liệu trong một thiết bị). Chứng cứ số sự cố ATTT có thể liên quan đến các máy tính hoặc hệ thống mạng.

B. Phương pháp thu thập chứng cứ số sự cố ATTT

Thu thập chứng cứ số là việc tạo ra một bản sao chính xác các chứng cứ hay còn gọi là nhân bản điều tra các vật chứa dữ liệu, xác định rõ các nguồn chứng cứ sau đó thu thập và bảo vệ tính toàn vẹn của chứng cứ bằng việc sử dụng hàm băm mật mã (sử dụng SHA1 hoặc MD5), phải được đưa vào một môi trường điều tra an toàn để phục vụ phân tích, điều tra sự cố. Trong quá trình thu thập chứng cứ cần phải xác minh độ chính xác của các bản sao thu được.

Các chứng cứ số trên hệ thống máy tính có thể bất biến (non-volatile data) hoặc khả biến (volatile data), mỗi loại chứng cứ đều đòi hỏi kỹ thuật thu thập khác nhau. Tuy nhiên, nên thu thập các chứng cứ khả biến trước vì chúng rất dễ bị mất, sau đó mới đến các chứng cứ bất biến vì chúng tồn tại trong thời gian dài trên hệ thống máy tính. Việc thu thập chứng cứ trên hệ thống này bao gồm việc thu thập trong RAM và thu thập trong các thiết bị nhớ ngoài (Disk).

Có 2 phương pháp thu thập chứng cứ số cơ bản, đó là: Đóng băng hiện trường (Freezing the scene) và Mồi nhử, hay còn gọi là Hũ mật (Honeypot) [1].

- *Đóng băng hiện trường:* Là việc thu thập dữ liệu của hệ thống bị sự cố. Tất cả các dữ liệu thu được từ hệ thống (bộ nhớ, tiến trình, kết nối mạng, phân vùng đĩa, …) phải được ghi lại và ký mã bởi các thuật toán như MD5 hoặc SHA1 để đảm bảo tính toàn vẹn chứng cứ. Việc thu thập dữ liệu nên bắt đầu từ những dữ liệu quan trọng trong các vật tải có thể tháo rời ở định dạng tiêu chuẩn.

- *Mồi nhử:* Là một hệ thống được xây dựng làm mồi nhử với mục đích dụ tin tặc vào đó để theo dõi, đồng thời ngăn không cho chúng tiếp xúc với hệ thống thật. Honeypot có thể giả dạng bất cứ loại máy chủ tài nguyên nào như Mail Server, Domain Name Server (DNS), Web Server,... Mồi nhử sẽ trực tiếp tương tác với tin tặc và tìm cách khai thác thông tin về chúng như hình thức tấn công, công cụ tấn công hay cách thức tiến hành tấn công. Có thể sử dụng linh hoạt một trong hai cách này, hoặc dùng cả hai cách cùng lúc tùy vào trường hợp cụ thể.

Để thu thập chứng cứ số trong RAM, có thể sử dụng phương pháp thu thập dựa trên phần cứng hoặc phần mềm. Việc thu thập chứng cứ dựa trên phần cứng thường đáng tin cậy và khó làm sai lệch chứng cứ, nhưng hiện tại việc thu lại bộ nhớ RAM dựa vào phần mềm thường được sử dụng vì nó có chi phí phù hợp, dễ tìm kiếm.

Thu thập chứng cứ số trong RAM dựa trên phần cứng liên quan đến việc tạm ngưng quá trình xử lý của máy tính và thực hiện truy cập bộ nhớ trực tiếp để có được một bản sao của bộ nhớ, nó được coi là tin cậy hơn vì ngay cả khi hệ điều hành và phần mềm trên hệ thống đã bị xâm nhập, hoặc bị làm sai lệch bởi tin tặc, ta vẫn có thể nhận

được một hình ảnh chính xác của bộ nhớ do không phụ thuộc vào các thành phần của hệ thống. Tuy nhiên, phương pháp này có nhược điểm là chi phí cao. Một trong các phần cứng chuyên dụng thiết kế cho mục đích này là Tribble Card, nó là một tấm mạch PCI được cài đặt sẵn trong hệ thống để ghi lại bộ nhớ một cách chính xác và đáng tin cậy nhất.

Thu thập chứng cứ số trong RAM dựa trên phần mềm là kỹ thuật sử dụng các bộ công cụ đáng tin cậy, được phát triển và cung cấp bởi các chuyên gia điều tra số hàng đầu trên thế giới như Memoryze, DumpIt, Win32dd, Mandiant Redline,… hoặc cũng có thể sử dụng những công cụ đã được tích hợp sẵn trong hệ thống để tiến hành thu lại bộ nhớ RAM như Memdump trong Linux. Thu thập chứng cứ số trên Disk là việc thu thập dữ liệu được lưu trữ trên phương tiện lưu trữ vật lý, nhằm trích xuất dữ liệu ẩn, khôi phục các tệp tin bị xóa, qua đó xác định người đã tạo ra những thay đổi dữ liệu trên thiết bị được phân tích. Các công cụ thường được sử dụng là DdRescue, dc3dd, Aimage.

Điều tra mạng liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính, cả LAN, WAN, Internet, nhằm mục đích thu thập bằng chứng hoặc phát hiện xâm nhập. Lưu lượng thường bị chặn ở cấp độ gói và được lưu trữ để phân tích sau này hoặc được lọc trong thời gian thực. Việc thu thập dữ liệu hệ thống mạng là việc thu các thông tin liên quan đến tình trạng hoạt động của các thiết bị trong hệ thống mạng. Có 2 phương pháp thu thập dữ liệu của hệ thống mạng, gồm: đẩy dữ liệu (push) , theo đó các sự kiện (event) từ các thành phần của hệ thống sẽ được tự động chuyển về các thành phần thu thập dữ liệu theo thời gian thực hoặc sau mỗi khoảng thời gian nhất định đã được cấu hình; trong khi đó lấy dữ liệu (pull), theo cách này các sự kiện phát sinh sẽ được lưu trữ trên chính các thành phần của hệ thống và sẽ được các thành phần thu thập dữ liệu chủ động lấy về. Một số công cụ hỗ trợ thu thập chứng cứ sự cố hệ thống mạng thường dùng, ví dụ như: Wireshark, Tcpdump, Network Miner, Snort,…

C. Phương pháp, kỹ thuật phân tích chứng cứ, xác định nguyên nhân sự cố máy tính

1. Phân tích dữ liệu chứng cứ số trong bộ nhớ chính

Phân tích, điều tra máy tính thực hiện bằng việc ghi lại bộ nhớ RAM tại thời điểm có dấu hiệu nghi ngờ hoặc đang bị tấn công để tiến hành phân tích, điều tra để việc xác định nguyên nhân sự cố cũng như các hành vi đã xảy ra trên hệ thống. Điều này được sử dụng khi quá trình phân tích tĩnh từ những gói tin thu được, cũng như các thông tin từ nhật ký hệ thống ghi lại, nhưng chưa xác định được nguồn gốc cũng như kỹ thuật tấn công hoặc cung cấp các thông tin có được chưa đầy đủ, chưa đủ sức thuyết phục. Cụ thể là kỹ thuật sử dụng kiến trúc quản lý bộ nhớ trong máy tính để ánh xạ, trích xuất các tệp tin đang thực thi và cư trú trong bộ nhớ vật lý của máy tính. Thực tế, bất kỳ thông tin nào tìm thấy trong bộ nhớ RAM, sẽ được hiểu là gần đây nó đã được chạy trên hệ thống của nạn nhân.

Các vết tích có liên quan đến RAM sau khi được xác định sẽ được coi là chứng cứ số cơ sở và được phân tích để khai thác những dấu hiệu của tội phạm. Sử dụng phương pháp thống kê và khai phá dữ liệu trên bộ nhớ chính để tìm kiếm những dữ liệu phù hợp với các mẫu tấn công, xâm nhập nghi ngờ. Một vài thông số quan trọng liên quan đến việc phân tích điều tra bộ nhớ chính như các thông tin được lưu trong RAM (tại thời điểm hệ thống hoặc máy tính đang hoạt động và có sự cố), các nhật ký sự kiện, thời gian, các kết nối mạng, truy vấn DNS, phân mảnh gói tin và các thông tin khác có liên quan đến bộ nhớ chính [2, 3]. Các mẫu chứng cứ được xâu chuỗi với nhau và thực hiện tấn công thử nghiệm để tái hiện lại hiện trường giúp xác định các phương thức, mục đích, hành động và thông tin liên quan đến kẻ tấn công. Kết quả của giai đoạn này là sự xác nhận các hành động khả nghi.

Một số kỹ thuật phân tích, phát hiện nguyên nhận sự cố mất ATTT trong bộ nhớ chính gồm: Phân tích bộ nhớ chính, nhật ký, dòng thời gian hệ thống và phân tích chuyên sâu. Công cụ phân tích có thể sử dụng gồm: NetworkMiner, Splunk, OllyDbg, Scapy, FTK Images, Process Explorer, Process Monitor,…

2. Phân tích các tiến trình đang chạy trên hệ thống

Tất cả các tiến trình đang chạy được lưu trữ ở bộ nhớ và có thể được lấy ra bằng việc sử dụng các công cụ dựa vào cấu trúc của hệ thống đang điều tra. Trong hệ điều hành có nhiều tiến trình khác nhau, tiến trình này có thể là tiến trình con hay tiến trình cha của tiến trình kia, tất cả những tiến trình đó có thể được tìm thấy trong bộ nhớ RAM. Các tiến trình ẩn cũng có thể được trích xuất ra khỏi bộ nhớ đã được ghi lại. Khi các tiến trình đã kết thúc nó vẫn có thể được cư trú trong bộ nhớ do không gian cư trú vẫn chưa được phân bổ lại [2, 6]. Volatility là công cụ tốt để phân tích các tiến trình.

3. Phân tích các tệp tin đang mở và Registry Handles

Các tệp tin đang mở cũng như bất kỳ một xử lý registry nào được truy xuất bởi một tiến trình đều được lưu trữ trong bộ nhớ. Thông tin về các tệp tin đang mở hay các xử lý liên quan đến Registry (giả sử có tiến trình của phần mềm độc hại đang chạy trên hệ thống thì các tệp tin đang mở có thể giúp phát hiện nơi mà mã độc hại đang được lưu trữ trên đĩa). Theo dõi Registry có thể đưa ra một cái nhìn quan trọng về các thông tin như nơi kết nối ra ngoài của mã độc, cách nó lưu trữ và kỹ thuật dùng để che dấu, cách hoạt động. Trong Windows thì Registry chứa rất nhiều thông tin có giá trị, là nơi có thể thu thập các chứng cứ rất hữu ích phục vụ cho công tác điều tra, còn đối với trong môi trường *NIX, các tệp tin được ánh xạ vào bộ nhớ thường được mô tả bởi một cấu trúc inode, lưu giữ thông tin về các tệp tin mà bộ nhớ ánh xạ, chẳng hạn như việc sửa đổi, truy cập cũng như thời gian thay đổi của tệp tin, như vậy với bất kỳ thông tin nào liên quan đến hệ thống đều có thể giúp người điều tra sử dụng để xác nhận các sự kiện đã được thiết lập [2, 6].

4. Phân tích các kết nối mạng đang có trong hệ thống

Thông tin về các kết nối mạng, bao gồm các cổng đang lắng nghe trên hệ thống, kết nối đang được thiết lập và thông tin liên kết giữa hệ thống với các kết nối từ xa, những thông tin này đều có thể được lấy ra từ bộ nhớ. Những thông tin về các kết nối mạng có thể cho biết các kết nối cửa sau trong hệ thống, các máy chủ điều khiển botnet,… dựa vào các kết nối của nó. Hầu hết các công cụ phân tích bộ nhớ hiện nay đều hỗ trợ việc liệt kê để xem nếu có kết nối ra ngoài hệ thống thì chúng thuộc về tiến trình nào, nếu là tiến trình của các trình duyệt web có thể là các kết nối bình thường, trong trường hợp có nhiều kết nối đến cổng 80 nhưng lại xuất phát từ tiến trình như ***svschost*** thì rõ ràng có vấn đề trong phiên kết nối đó [7, 8].

5. Phân tích mật khẩu và khóa mật mã

Thực hiện phân tích điều tra bộ nhớ để phục hồi mật khẩu người dùng và các khóa mật mã có thể được dùng để giải mã các tệp tin, chương trình mà người dùng sử dụng, truy cập. Mật khẩu, khóa mật mã được lưu trữ trong bộ nhớ RAM, nên khi phân tích, điều tra bằng việc ghi lại bộ nhớ RAM có thể giúp phục hồi dữ liệu, khôi phục mật khẩu và có thể truy cập vào tài khoản trực tuyến của người đang bị điều tra như thư điện tử và dữ liệu lưu trữ [2, 3].

6. Phân tích kiểu xếp chồng dữ liệu chứng cứ sự cố ATTT

Xếp chồng dữ liệu là ứng dụng của phân tích tần số cho khối lượng lớn dữ liệu tương tự nhằm cố gắng cô lập và xác định các điểm bất thường. Nó liên quan đến một quá trình lặp đi lặp lại để giảm lượng lớn dữ liệu thành các phần có thể quản lý được để có thể sử dụng và điều tra. Theo FireEye, tổ chức của Hoa Kỳ thường xuyên điều tra sự cố ATTT với hàng trăm nghìn máy chủ, việc xem xét dữ liệu này mà không xử lý trước và giảm thiểu, chẳng hạn như xếp chồng dữ liệu, là không khả thi. Họ thường sử dụng tính năng xếp chồng dữ liệu để phát hiện phần mềm độc hại không xác định và các chỉ số dấu hiệu xâm nhập (Indicator of Compromise - IoC) mới trong quá trình điều tra của mình [9].

Khi điều tra các cuộc tấn công có chủ đích, dữ liệu độc hại ít phổ biến hơn trong toàn doanh nghiệp so với dữ liệu lành tính, cho phép các nhà điều tra tập trung nỗ lực vào các hàng kiểm tra có vẻ khác nhau. Với một tập hợp dữ liệu lớn, người điều tra xác định những thuộc tính nào làm cho các hàng dữ liệu bất thường trở nên nổi bật và có thể chỉ ra rằng chúng là độc hại. Các thuộc tính này sau đó trở thành tiêu chí phân nhóm được sử dụng để tạo các phép tính phân tích tần suất. Sau đó, tần suất hoặc số lượng được sử dụng để xác định điểm bắt đầu điều tra cho các bất thường có thể xảy ra trong doanh nghiệp.

7. Phân tích kiểu đánh giá theo dòng thời gian timeline

Dòng thời gian là kỹ thuật hiển thị danh sách các sự kiện theo một thứ tự cụ thể. Phân tích dòng thời gian chủ yếu được sử dụng cho các mục tiêu khác nhau trong cuộc điều tra, chủ yếu liên quan đến việc thu thập thông tin trong một khung thời gian cụ thể. Đó là một kỹ thuật tốt để xác định hoạt động bất thường xảy ra trên một hệ thống tại một thời điểm nhất định. Phân tích dòng thời gian thông thường để điều tra pháp lý máy tính có thể được thực hiện trên các loại bối cảnh khác nhau, như dòng thời gian văn bản, dòng thời gian số, dòng thời gian đồ họa,... Mỗi mô hình dòng thời gian cung cấp các chế độ xem dữ liệu khác nhau cho phù hợp. Thông qua phân tích dòng thời gian, nhà phân tích có thể dễ dàng tìm ra thời điểm một sự kiện hoặc giao dịch cụ thể đã xảy ra. Nó cũng giúp tìm ra các sự kiện khác diễn ra trong cùng một khoảng thời gian cùng với sự liên kết của chúng với nhau [10].

8. Phân tích phát hiện mã độc

Việc xác định nguyên nhân sự cố được nhóm tác giả quan tâm đầu tiên đến khả năng liệu có mã độc trong máy tính bị sự cố hay không. Các tệp dữ liệu có khả năng chứa mã độc sẽ được thu thập từ máy tính bị sự cố, chẳng hạn như các tệp tin hệ thống, các tệp được tải xuống bởi trình duyệt,…

Để phân tích, xác định nguyên nhân sự cố thông qua dò quét mã độc trong tệp dữ liệu chứng cứ được thực hiện như sau: Từ những tệp chứng cứ đã thu thập được, phân hệ chức năng sẽ kết hợp các hàm API của phần mềm multiAV để tiến hành phân tích, rà quét và tìm kiếm mã độc trong tệp tin giúp nhà phân tích rút ngắn thời gian phân tích, nhanh chóng xác định được nguyên nhân của sự cố.

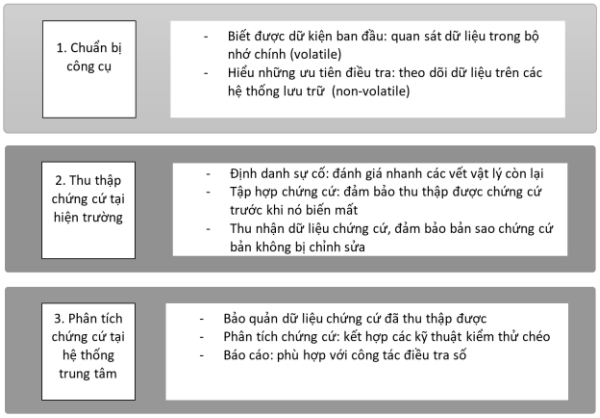
9. Phân tích sử dụng danh sách đen

Để xác định nguyên nhân và đưa ra tư vấn, gợi ý hỗ trợ, nhóm tác giả đã xây dựng một tập dữ liệu về các nguy cơ, cảnh báo có thể xảy ra. Các dữ liệu bao gồm: Tập các tệp nghi ngờ có mã độc; Tập địa chỉ IP đen; Các mục registry đen; Các tiến trình mã độc; Các sự kiện đen,…

III. GIẢI PHÁP HỖ TRỢ XỬ LÝ RỦI RO AN TOÀN CÁC HỆ THỐNG CNTT

Trong khuôn khổ nghiên cứu này, giải pháp hỗ trợ xử lý sự cố an toàn các hệ thống CNTT được xây dựng bao gồm: (i) Quy trình xử lý sự cố ATTT và (ii) Hệ thống phần mềm cung cấp các chức năng để thực hiện được các bước trong quy trình đó. Hai thành phần của giải pháp này sẽ được trình bày cụ thể ở các mục sau đây.

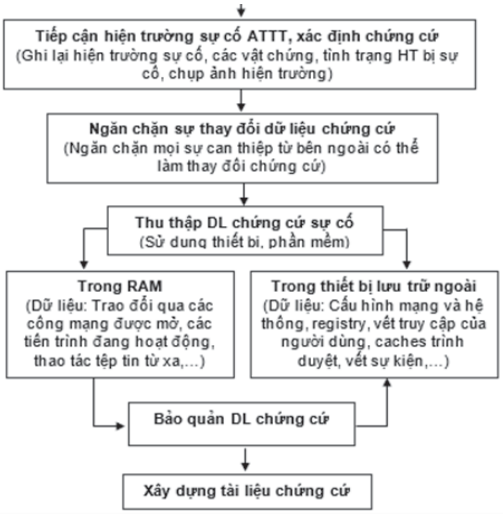
A. Quy trình hỗ trợ xử lý sự cố an toàn các hệ thống CNTT



Hình 1. Quy trình tổng thể hỗ trợ xử lý sự cố an toàn các hệ thống CNTT

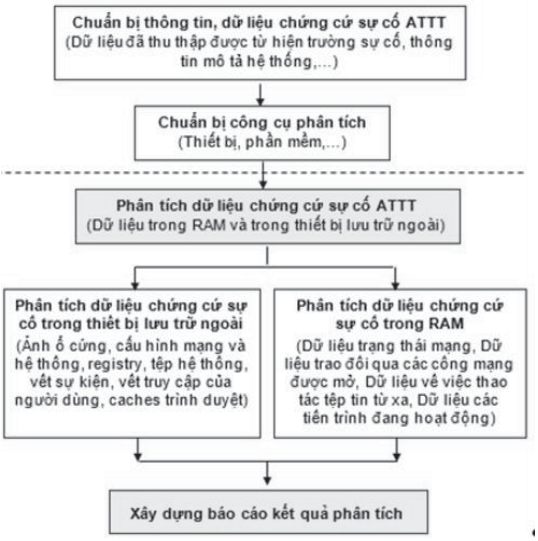
Trên cơ sở tiêu chuẩn ISO/IEC 27035 [12] về quản lý sự cố ATTT, quy trình tổng thể xử lý sự cố an toàn các hệ thống CNTT gồm 3 bước chính như trong Hình 1.

Hoạt động thu thập và bảo quản dữ liệu chứng cứ được thực hiện theo các bước trong Hình 2 [13,15] (Tương ứng với bước 2 trong quy trình tổng thể).



Hình 2. Quy trình thu thập chứng cứ số sự cố ATTT

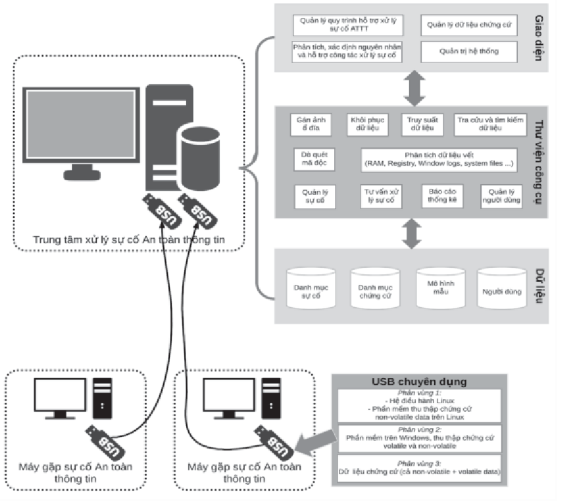
Đối với bước 3 trong quy trình tổng thể, việc phân tích dữ liệu chứng cứ số sự cố ATTT được thể hiện qua Hình 3 với quy trình gồm các bước sau [14, 15]:



Hình 3. Quy trình phân tích chứng cứ số sự cố ATTT

B. Mô hình kiến trúc hệ thống hỗ trợ xử lý sự cố an toàn các hệ thống CNTT

Hệ thống hỗ trợ xử lý sự cố an toàn các hệ thống CNTT (gọi tắt là UET.SIR - Security Incident Response System) được xây dựng dựa trên theo quy trình xử lý sự cố ATTT, gồm 2 giai đoạn chính: (i) Thu thập chứng cứ sự cố ATTT và (ii) Phân tích chứng cứ sự cố.



Hình 4. Mô hình kiến trúc hệ thống hỗ trợ xử lý sự cố an toàn các hệ thống CNTT

Hệ thống này bao gồm 2 thành phần tương ứng với 2 giai đoạn chính trong công tác ứng cứu, xử lý sự cố ATTT:

- Thành phần hỗ trợ thu thập chứng cứ sự cố ATTT: Bao gồm một USB chuyên dụng có định dạng dữ liệu chuyên biệt chống nguy cơ lây nhiễm ngược, cùng với phần mềm công cụ phục vụ cho công tác thu thập chứng cứ sự cố ATTT.

- Thành phần hỗ trợ phân tích chứng cứ sự cố: Đây là Phần mềm trung tâm với các phân hệ: Quản lý quy trình hỗ trợ xử lý sự cố ATTT; Quản lý dữ liệu chứng cứ sự cố ATTT; Phân tích, xác định nguyên nhân hỗ trợ công tác xử lý sự cố ATTT; Quản trị hệ thống kèm theo Thư viện công cụ, các cơ sở dữ liệu.

Các chức năng chính của Hệ thống hỗ trợ xử lý sự cố ATTT được minh hoạ như Hình 4.

C. USB chuyên dụng phục vụ thu thập dữ liệu sự cố ATTT

Giải pháp thu thập dữ liệu sự cố ATTT được nhóm tác giả tiếp cận theo cách sử dụng USB chuyên dụng. USB này cơ bản có thể dùng USB thương mại nhưng được tổ chức định dạng dữ liệu chuyên biệt để chống nguy cơ lây nhiễm ngược. USB được tổ chức với 3 phân vùng chính như sau:

- Phân vùng 1 chứa hệ điều hành Linux chuyên dụng: Được tuỳ biến từ Kali Linux, có chứa phần mềm công cụ hỗ trợ thu thập dữ liệu chứng cứ trong bộ nhớ chính (volatile data) của máy tính bị sự cố ATTT. Phân vùng này được cài đặt cơ chế chống ghi ngược từ hệ thống khác và được mã hoá với AES-256; chỉ có thể cập nhật từ phía phần mềm trung tâm.

- Phân vùng 2 chứa phần mềm công cụ chạy trên Windows: Phục vụ việc thu thập dữ liệu chứng cứ trong cả bộ nhớ chính (volatile data) lẫn trong thiết bị lưu trữ (non-volatile data) của máy tính bị sự cố ATTT. Phân vùng này cũng được cài đặt cơ chế chống ghi ngược với phương pháp thiết lập chỉ đọc, mã hoá với cơ chế Bitlocker, chứa IncidentCollector.iso. Phần mềm này cũng chỉ có thể cập nhật từ phía phần mềm trung tâm.

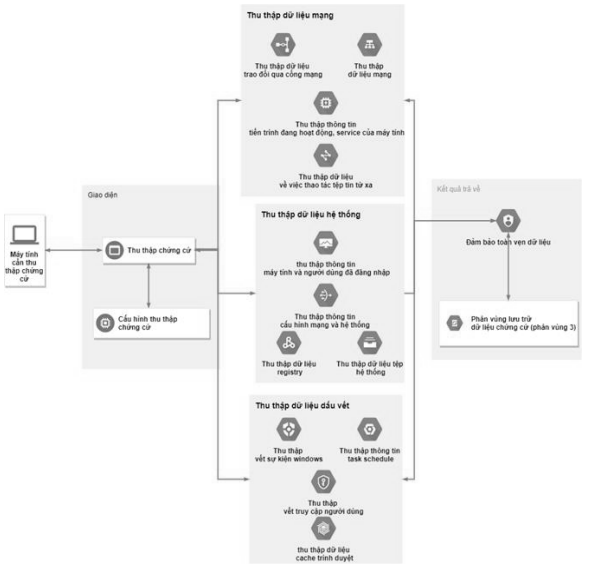
- Phân vùng 3 dùng để lưu tạm thời dữ liệu chứng cứ đã thu thập được theo cả hai phương pháp nêu trên: Phân vùng này có cơ chế đảm bảo tính toàn vẹn của toàn bộ dữ liệu chứng cứ thu thập được.

Để chống nguy cơ lây nhiễm ngược cho USB, cần phải có cơ chế chống ghi vào các phân vùng USB hoặc phát hiện việc ghi trái phép vào phân vùng để dừng việc sử dụng USB đó. Chống ghi ngược USB có thể được thực hiện thông qua USB chuyên dụng hoặc dùng phần mềm để ngăn tạo

mới/cập nhật dữ liệu. Cách tiếp cận của nhóm tác giả để giải quyết vấn đề này là sử dụng mật mã học [15].

D. Công cụ thu thập dữ liệu chứng cứ sự cố IncidentCollector

Công cụ thu thập dữ liệu chứng cứ sự cố được xây dựng theo mô hình kiến trúc được thể hiện trong Hình 5.



Hình 5. Kiến trúc công cụ thu thập dữ liệu sự cố ATTT

Đối với dữ liệu sự cố ATTT, các loại dữ liệu dấu vết, dữ liệu hệ thống, dữ liệu mạng, do để dễ dàng hơn trong việc phân tích, điều tra chứng cứ, cần thu thập có chọn lọc và chuyển dữ liệu sang dữ liệu XML. Còn đối với dữ liệu cache trình duyệt, do dữ liệu khá lớn và các tệp tin nghi ngờ bất thường, có thể có mã độc được nhóm tác giả lấy nguyên trạng từ máy tính.

E. Phần mềm trung tâm

Phần mềm trung tâm bao gồm: Các phân hệ ứng dụng hỗ trợ xử lý sự cố ATTT và Thư viện công cụ.

1. Các phân hệ ứng dụng hỗ trợ xử lý sự cố ATTT

Các phân hệ ứng dụng hỗ trợ xử lý sự cố ATTT gồm các phân hệ sau:

- Phân hệ quản lý quy trình hỗ trợ xử lý sự cố ATTT: Gồm 2 mô-đun, đó là mô-đun quản lý các quy trình xử lý sự cố ATTT và mô-đun quản lý các mẫu xử lý sự cố ATTT.

- Phân hệ quản lý dữ liệu chứng cứ sự cố ATTT: Đảm nhiệm vai trò tiếp nhận toàn bộ dữ liệu chứng cứ đã thu thập được và lưu trong các USB chuyên dụng. Phân hệ này có khả năng hỗ trợ khôi phục dữ liệu từ ảnh ổ đĩa đã thu thập, tiếp nhận dữ liệu bị hỏng bảng định vị tệp tin,… Ngoài ra, còn có các chức năng hỗ trợ tìm kiếm thông tin trên toàn bộ dữ liệu chứng cứ, cho phép quản lý và tra cứu danh mục chứng cứ thu thập được.

- Phân hệ phân tích, xác định nguyên nhân và hỗ trợ công tác xử lý sự cố ATTT: Đảm nhiệm chức năng phân tích, xác định nguyên nhân, từ đó hỗ trợ công tác xử lý sự cố ATTT.

- Phân hệ quản trị hệ thống.

2. Thư viện chức năng

Thư viện chức năng có vai trò cung cấp các công cụ hệ thống bên dưới để từ đó các ứng dụng, dịch vụ ở mức trên có thể khai thác, sử dụng để thi hành các chức năng theo thiết kế. Các công cụ hệ thống phía dưới bao gồm: Gán ảnh ổ đĩa; Khôi phục dữ liệu; Truy xuất dữ liệu; Tra cứu và tìm kiếm dữ liệu; Dò quét mã độc; Phân tích dữ liệu vết; Quản lý sự cố; Tư vấn xử lý sự cố; Quản lý người dùng; Báo cáo thống kê.

IV. Thực nghiệm

Dựa trên giải pháp đã đề xuất ở mục III và kết quả xây dựng hệ thống ở mục IV, nhóm tác giả đã hình thành được hệ thống hỗ trợ xử lý sự cố ATTT, gọi tắt là UET.SIR và triển khai thử nghiệm tại Bộ Tài nguyên và Môi trường.

A. Môi trường thử nghiệm

Hệ thống trung tâm UET.SIR đã được triển khai tại máy chủ đặt tại trung tâm dữ liệu của Cục CNTT và Dữ liệu tài nguyên môi trường (Bộ Tài nguyên và Môi trường). Thông tin máy chủ cài đặt hệ thống này như sau: 12 cores Xeon Gold 6118; RAM: 32GB; Storage: 200GB; thư viện công cụ: nginx 1.18, elastisearch 7.1, postgresql 12.6.

Các công cụ phân tích nền đã được nhóm tác giả triển khai cài đặt tại máy chủ trên. Dịch vụ backend của hệ thống UET.SIR cũng được triển khai tại địa chỉ *https://sirapi.dinte.vn/*.

Dịch vụ frontend của hệ thống UET.SIR triển khai tại Bộ Tài nguyên và Môi trường sẽ cho phép người dùng truy cập tại địa chỉ *https://sir.dinte.vn/*.

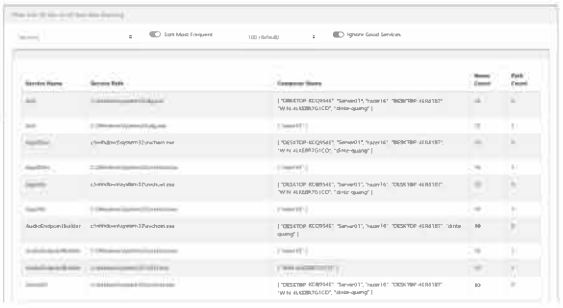
Kịch bản thử nghiệm bao gồm sử dụng USB chuyên dụng để thu thập dữ liệu sự cố ATTT trên các máy tính của người dùng đang còn hoạt động, và

máy tính người dùng đã tắt để tiến hành phân tích, tìm ra nguyên nhân sự cố và khuyến nghị xử lý.

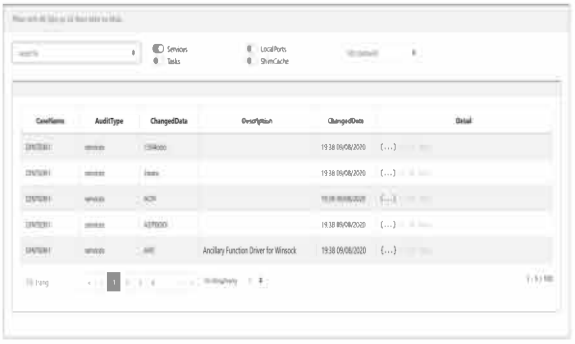
B. Kết quả xây dựng UET.SIR

Toàn bộ các chức năng của hệ thống UET.SIR được đặc tả trong giải pháp ở phần III đã hoàn thành và vận hành đáp ứng được những yêu cầu đặt ra. Một số chức năng chính của UET.SIR được minh hoạ ở các hình sau:

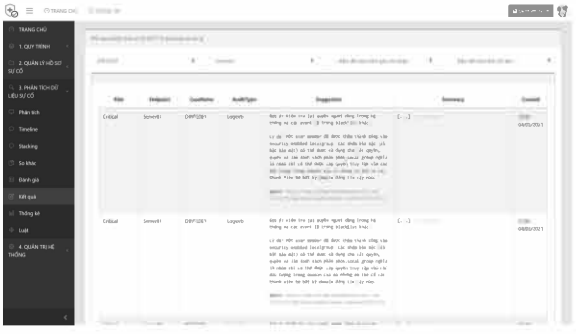
Hình 6. Chức năng Phân tích Timeline



Hình 7. Chức năng Phân tích xếp chồng Stacking



Hình 8. Chức năng Phân tích so khác



Hình 9. Kết quả phân tích dữ liệu chứng cứ sự cố ATTT của máy chủ "Server01"

C. Đánh giá

1. USB chuyên dụng chứa phần mềm thu thập dữ liệu sự cố ATTT

So sánh USB chuyên dụng trong nghiên cứu này với các sản phẩm USB chuyên dụng khác như Bootable USB của hãng PassMark cho thấy có được các chức năng tương tự, cụ thể như sau:

- *Có khả năng khởi động trực tiếp từ USB:* Trong bài báo sử dụng hệ điều hành Kali Linux được tuỳ biến, trong khi USB PassMark sử dụng Windows PE.

- *Có công cụ thu thập dữ liệu sự cố ATTT:* UET.SIR chỉ sử dụng USB để thu thập dữ liệu sự cố, toàn bộ phần phân tích, xử lý được thực hiện trên trung tâm. Với PassMark thì cho phép thu thập và phân tích dữ liệu sự cố ATTT trực tiếp trên USB với phần mềm chạy trên Windows.

2. Phần mềm hỗ trợ phân tích, xử lý sự cố ATTT

Dựa vào tài liệu của các phần mềm Security Resilient của hãng IBM, Mandiant của hãng FireEye hay Encase, FTK, nhóm tác giả đã tìm hiểu và tiến hành so sánh về mặt chức năng. Kết quả được thể hiện như trên Bảng 1.

V. KẾT LUẬN

Trong bài báo này, nhóm tác giả đã trình bày giải pháp hỗ trợ xử lý sự cố an toàn thông tin đối với các hệ thống thông tin nói chung và Chính phủ điện tử nói riêng. Giải pháp này dựa trên bộ quy trình quy trình hỗ trợ xử lý sự cố ATTT trong Chính phủ điện tử được tuỳ biến trên cơ sở các tiêu chuẩn TCVN 11239:2015, TCVN ISO/IEC 27037:2019, ISO/IEC 27035-2011 và NIST SP800-61 cùng với hệ thống hỗ trợ xử lý sự cố ATTT UET.SIR, bao gồm USB chuyên dụng chứa công cụ thu thập được những dữ liệu chứng cứ sự cố ATTT quan trọng, và phần mềm trung tâm cung cấp các chức năng để phân tích dữ liệu sự cố (phân tích mã độc, phân tích theo kiểu xếp chồng, so khác,…). Phần mềm trung tâm này có chức năng tương tự với một số sản phẩm thương mại của các tập đoàn, đã thử nghiệm thực tế tại Bộ Tài nguyên và Môi trường. Các kết quả bước đầu thu được đã minh chứng kết quả của sản phẩm, hỗ trợ hiệu quả cho công tác đảm bảo ATTT tại cơ quan nhà nước

BẢNG 1. SO SÁNH, ĐÁNH GIÁ CHỨC NĂNG CỦA UET.SIR VÀ MỘT SỐ SẢN PHẨM KHÁC

Chức năng	UET.SIR	Mandiant	IBM Resilent	Encase	FTK
Quản lý hồ sơ, máy tính và dữ liệu sự cố	Có, theo mô hình phân cấp	Có	Có	Có	Có
Phân tích chuyên biệt pháp lý số	Không	Không	Không	Có	Có
Phân tích dữ liệu tìm bất thường	Có	Có	Có	Không	Không
Phân tích kiểu timeline	Có	Có	Có	Có	Có
Phân tích kiểu stacking	Có	Có	Không	Không	Không
Báo cáo, thống kê	Có	Có	Có	Không	Không
Mô hình triển khai	Web	Desktop	Web	Desktop	Desktop

Trong thời gian tới, nhóm tác giả sẽ tiếp tục hoàn thiện thêm hệ thống phần mềm, bổ sung những chức năng phân tích chuyên sâu để hỗ trợ công tác xử lý sự cố ATTT cho các hệ thống CNTT trong Chính phủ điện tử tại Việt Nam.

VI. TÀI LIỆU THAM KHẢO

[1]. T. Sethi and R. Mathew, "A Study on Advancement in Honeypot based Network Security Model," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 94-97.

[2]. Ồn, P. V., Hà, L. V., & Hóa, N. N. (2022). Giải pháp đánh giá và quản lý rủi ro an toàn thông tin trong Chính phủ điện tử. Journal of Science and Technology on Information Security, 1(13), 35-48. https://doi.org/10.54654/isj.v1i13.144

[3]. Shiva V. N Parasram (2017): Digital Forensics with Kali Linux. Packt Publisher.

[4]. Ir – Rescue, URL: https://github.com/diogo-fernan/ir-rescue.

[5]. S. B. Deb and A. Chetry, "USB Device Forensics: Insertion and removal timestamps of USB devices in Windows 8," 2015 International Symposium on Advanced Computing and Communication (ISACC), Silchar, 2015, pp. 364-371.

[6]. Sajedul Talukder1 (2020), Tools and Techniques for Malware Detection and Analysis.

[7]. Abhishek Srivastav, Irman Ali (2014), "Network Forensics an emerging approach to an network analysis", International Journal of Computer Science & Engineering Technology (IJCSET). Vol. 5 No. 02 Feb 2014, pp 118-123.

[8]. Samir Datt (2016), Learning Network Forensics. Packt Publishing, Birmingham, UK

[9]. M. Cohen, "Forensic analysis of windows user space applications through heap allocations," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 237-244.

[10]. Y.C. Liao and H. Langweg, "Events and causal factors charting of kernel traces for root cause analysis," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 245-250.

[11]. Sajedul Talukder1 and Zahidur Talukder, A survey on malware detection and analysis tools, International Journal of Network Security & Its Applications (IJNSA) Vol. 12, No.2, March 2020, pp 37-57.

[12]. ISO/IEC 27035:2016— Information technology — Security techniques — Information security incident management.

[13]. ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.

[14]. ISO/IEC 27042:2015— Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.

[15]. Nguyễn Ngọc Hóa, Phùng Văn Ồn (2021): Báo cáo tổng hợp kết quả đề tài nghiên cứu cấp Quốc gia về "Nghiên cứu, xây dựng hệ thống đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố an toàn thông tin trong chính phủ điện tử", mã số KC01.19/16-20.

[16]. Lê Hồng Hải, Phùng Văn Ồn, Tống Minh Đức, Ngô Quang Huy, Nguyễn Ngọc Hóa, "UET.SIR: Giải pháp hỗ trợ xử lý sự cố an toàn thông tin trong chính phủ điện tử", kỷ yếu hội thảo Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông", 2021.

VII. SƠ LƯỢC VỀ TÁC GIẢ

Lê Hồng Hải

Đơn vị công tác: Khoa Công nghệ thông tin, Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội.

Email: hailh@vnu.edu.vn

Quá trình đào tạo: Tốt nghiệp Đại học ngành Máy tính tại Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội vào năm 1981; Thạc sĩ năm 2007 và Tiến sĩ năm 2018 chuyên ngành Hệ thống thông tin tại Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội.

Hướng nghiên cứu hiện nay: Hệ thống thông tin; an toàn thông tin; nhận dạng mẫu; phân tích dữ liệu.

Tống Minh Đức

Đơn vị công tác: Khoa Công nghệ thông tin, Học viện Kỹ thuật Quân sự.

Email: ductm@mta.edu.vn

Quá trình đào tạo: Tốt nghiệp Đại học ngành Công nghệ thông tin tại Học viện Kỹ thuật Quân sự vào năm 2000; Tiến sĩ chuyên ngành Tự động hóa và điều khiển các quy trình công nghệ sản xuất tại Trường Đại học Tổng hợp Kỹ thuật Điện Xanh Petecbua – Liên bang Nga vào năm 2007.

Hướng nghiên cứu hiện nay: Hệ thống thông tin; an toàn thông tin; blockchain; big data.

Ngô Quang Huy

Đơn vị công tác: Trung tâm Thông Tin - Bộ Thông tin và Truyền thông.

Email:ngoquanghuy@gmail.com

Quá trình đào tạo: Tốt nghiệp Đại học chuyên ngành Toán tin ứng dụng tại Trường Đại học Bách khoa Hà nội năm 2000; Thạc sĩ Tin học năm 2006 tại Viện Tin học Pháp ngữ (IFI), Trường Đại Học Bách Khoa Hà nội.

Hướng nghiên cứu hiện nay là: Các giải pháp giám sát, phòng, chống tấn công mạng; kiến trúc và các quy trình bảo đảm ATTT cho tổ chức; chuyển đổi số.

Phùng Văn Ổn

Đơn vị công tác: Viện Công nghệ thông tin, Trường Đại học Tài chính – Ngân hàng Hà Nội.

Email: onphungvan@gmail.com

Quá trình đào tạo: Tốt nghiệp Đại học ngành Máy tính tại Trường Đại học Tổng hợp Hà Nội vào năm 1980; Thạc sĩ năm 1997 và Tiến sĩ năm 2001 chuyên ngành Bảo đảm toán học cho máy tính và hệ thống tính toán tại Trường Đại học Khoa học Tự nhiên - Đại học Quốc gia Hà Nội.

Hướng nghiên cứu hiện nay: Hệ thống thông tin; an toàn thông tin; chính phủ điện tử; giao thông thông minh.

Nguyễn Ngọc Hóa

Đơn vị công tác: Khoa Công nghệ thông tin, Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội.

Email: hoas.nguyen@gmail.com

Quá trình đào tạo: Tốt nghiệp Đại học ngành Khoa học máy tính tại Trường Đại học Bách khoa học Hà Nội vào năm 1999; Tiến sĩ ngành Khoa học máy tính tại Trường Đại học Joseph Fourier - Cộng hòa Pháp vào năm 2005.

Hướng nghiên cứu hiện nay: Hệ tích hợp thông minh; an toàn thông tin; quản lý dữ liệu lớn.